UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/982,711	10/18/2001	Taizo Shirai	09812.0590-00000	8666

22852 7590 11/03/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte TAIZO SHIRAI, YOSHIHITO ISHIBASHI, KENJI YOSHINO, TORU AKISHITA, TAKESHI ITO, and SHIGEKAZU HAYASHI

Appeal 2008-1081
Application 09/982,711
Technology Center 2400

Decided: November 3, 2008

Before ALLEN R. MACDONALD, ST. JOHN COURTENAY III, and THU A. DANG, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from a final rejection of claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32. Claims 2-4, 7, 9-11, 14, 18-20, 23, 25-27, and 30 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

A. INVENTION

According to Appellants, the invention relates to an information recording device, an information playback device, and information recording method, and an information playback method in which content stored in a storage device is protected under high security management, and an information recording medium and a program providing medium which are used therewith (Spec., p. 1, ll. 6-15).

B. ILLUSTRATIVE CLAIM

Claim 1 is exemplary and is reproduced below:

1. An information recording device for executing processing which stores data to a memory having a data storage area consisting of a plurality of blocks, each of the blocks consists of M sectors from a first sector to a M-th sector with each sector having a predetermined data capacity, where M represents a natural number, said information recording device comprising:

a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors;

wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information; and

an integrity checking unit for checking the integrity of the revocation list and the block permission table.

C. REJECTIONS

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Dilkie	US 6,341,164 B1	Jan. 22, 2002
Hazard	US 6,658,566 B1	Dec. 2, 2003
Sudia	US 2005/0114666 A1	May 26, 2005 (filed Sep. 24, 2004)

Claims 1, 5, 8, 12, 15-17, 21, 24, 28, 31, and 32 stand rejected under 35 U.S.C. § 103(a) over the teachings of Hazard and Sudia; and

Claims 6, 13, 22, and 29 stand rejected under 35 U.S.C. § 103(a) over the teachings of Hazard, Sudia, and Dilkie.

We affirm.

II. ISSUE(S)

The issue is whether Appellants have shown that the Examiner erred in finding that claims 1, 5, 8, 12, 15-17, 21, 24, 28, 31, and 32 are unpatentable under 35 U.S.C. § 103(a) . In particular, the issues are whether the combination of Hazard and Sudia discloses A) "a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors"; B) "wherein the data includes a revocation list having revocation information regarding revoked media or content and a block

permission table for accessing a permission table that describes memory access control information"; and C) "an integrity checking unit for checking the integrity of the revocation list and the block permission table" (Claim 1).

III. FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

Hazard

1. Hazard discloses storing and using sensitive information in a security module, wherein "security module" designates a device which can take the form of a portable device comprising a chip card, such as a bank card (col. 1, ll. 47-49).
2. A number n of temporary protection keys CP1, ... CPi, … CPn respectively include a key number N1, … Ni, … Nn used to designate them (col. 5, ll. 1-4, Fig. 2).
3. Each of a number m of items of sensitive information IS1, IS2, … IS(j-1), ISj, … Ism is stored in the security module in encrypted form using an encryption algorithm and a temporary protection key chosen (col. 5, ll. 15-20, Fig. 3).
4. Temporary protection key CP1 (whose number is N1) is used to protect the sensitive information IS1, IS2, the temporary protection key CPi is used for the sensitive information IS(j-1), and the

temporary protection key CPn is used for the sensitive information ISm only (col. 5, ll. 22-27, Figs. 2-3).

Sudia

5. Sudia discloses controlling access to data and network resources (p. 1, [0003]), wherein a server resumes or refuses (or cancels) the client's access to content governed by a given privilege, based on verification results (p. 17, [0362]).

6. A long list is compiled containing all possible authorizations, restrictions, and incorporated contract terms that might ever be desired to be granted to or imposed on the user (p. 10, [0228]).

7. An organization creates a table or list of possible authorizations for a given user (p. 11, [0237]).

8. A Freshness Service will, upon receipt of notification of revocation or suspension of a certificate or signature that was checked by a recipient/verifier, and push a notice of the revocation back to the recipient/verifier (p. 9, [0209]).

IV. PRINCIPLES OF LAW

35 U.S.C. § 103(a)

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007).

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," *Id.* at 1739, and discussed circumstances in which a patent might be determined to be obvious. *KSR,* 127 S. Ct. at 1739 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

The Federal Circuit recently recognized that "[a]n obviousness determination is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (citing *KSR*, 127 S. Ct. 1727, 1739 (2007)). The Federal Circuit relied in part on the fact that Leapfrog had presented no evidence that the inclusion of a reader in the combined device was "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Id.*1162 (citing *KSR*, 127 S. Ct. at 1740-41).

Claim Construction

"Our analysis begins with construing the claim limitations at issue." *Ex Parte Filatov*, No. 2006-1160, 2007 WL 1317144, at *2 (BPAI 2007).

"The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)). "Claims must be read in view of the specification, of which they are a part." *Markman v. Westview Instruments, Inc.,* 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc). "[T]he PTO gives claims their 'broadest reasonable interpretation.'" *In re Bigio*, 381 F.3d 1320, 1324 (Fed. Cir. 2004) (quoting *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000)). "Moreover, limitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citing *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989)).

When descriptive material is not functionally related to the substrate, the descriptive material will not distinguish the invention from the prior art in terms of patentability. *In re Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004). Cf. *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983).

V. ANALYSIS

Combinability under 35 U.S.C. § 103

The Examiner finds that one of ordinary skill in the art would have found it obvious to combine the teachings of the cited references beginning

at page 4 of the Answer. The Appellants provide no argument to dispute that the Examiner has correctly shown that it would have been obvious to combine the references. Thus, we deem those arguments waived.

Claims 1, 8, 15, 17, 24, 31, and 32

Appellants do not provide separate arguments with respect to the rejection of independent claims 1, 8, 15, 17, 24, 31, and 32. Therefore, we select independent claim 1 as being representative of the cited claims. 37 C.F.R. § 41.37(c)(1)(vii).

A. The cited references disclose "a different encryption key for each sector"

Appellants argue that "[c]onversely to sector level encryption [as set forth in Appellants' Specification], Hazard discloses data encryption at the file level" (App. Br. 8). Appellants further argue that "Hazard discloses the use of a temporary protection key based upon the sensitive information (IS) and not based upon a sector" (App. Br. 9), and that "IS1 and IS2 of Hazard is encrypted using the same encryption key, 'CP1.'" (App. Br. 10).

Appellants' argument that Hazard does not disclose "sector level encryption" because "Hazard discloses data encryption at the file level" is not commensurate with the claimed invention. That is, Appellants' claims do not recite any such "sector level encryption" and thus such argument is not commensurate with the invention that is claimed. Claims limitations are not to be read into the claims from the specification. *See In re Van Geuns*, 988 F.2d at 1184

Similarly, Appellants' arguments that Hazard's use of a temporary protection key is "based upon the sensitive information (IS) and not based upon a sector" and that "IS1 and IS2 of Hazard is encrypted using the same encryption key" also are not commensurate with the claimed invention. The claims do not recite any such "based upon a sector" limitation, but rather that "a different encryption key" is used "*for* each sector" (emphasis added) (claim 1). Appellants appear to be arguing that, because Hazard also uses an encryption key for each sensitive information, Hazard does not disclose *only* using an encryption key for each sector. However, such "*only* using" limitation is not recited in the claims and thus is not commensurate with the claimed invention. For similar reason, Appellants' apparent argument that because IS1 and IS2 of Hazard are encrypted using the same encryption key, Hazard does not disclose *only* using a different encryption key for each sector, also is not commensurate with the claimed invention.

Accordingly, the issue is whether Hazard discloses "a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors" (Claim 1).

We agree with the Examiner's finding that Hazard discloses such claimed limitation beginning at page 3 of the Answer, and the Examiner's corresponding responsive arguments beginning at page 14 of the Answer.

Hazard discloses storing and using sensitive information in a security module, which can take the form of a portable device comprising a chip card, such as a bank card (FF 1). In Hazard, sensitive information IS1, IS2, … IS(j-1), ISj, … Ism stored in the security module is encrypted using temporary protection keys CP1, ... CPi, … CPn with key numbers N1, … Ni, … Nn, wherein the temporary protection key CP1 (whose number is N1) is used to protect the sensitive information IS1, IS2, the temporary protection key CPi is used for the sensitive information IS(j-1), and the temporary protection key CPn is used for the sensitive information ISm (FF 2-4). The Examiner finds that "the term 'sector' [is given] its broadest reasonable interpretation," and that "Examiner believes that Hazard teaches the limitations of using a different encryption/decryption key for each sector from the first sector to the M-th sector" (Ans. 15). We generally agree.

We find that Hazard teaches that the sensitive information is stored in chip card of a security module (FF 1), wherein a particular encryption/decryption key (CP1) is used to protect certain sensitive information IS1, IS2 in the chip card, while a different key (CPi) is used to protect another sensitive information IS(j-1), and another different key (CPm) is used to protect yet another sensitive information Ism (FF 2-4). In particular, we find that the chip card of Hazard comprises sectors to store the sensitive information, wherein the information is stored using different encryption/decryption keys. We construe the term "sector" by giving the

term its customary and ordinary meaning, as "a part or division." In fact, as admitted by Appellants "a 'sector' refers to an allocated area of a storage medium" (Reply Br. 3).

Thus, we find that Hazard teaches, or at the least, strongly suggests, that a different encryption/decryption key (CP1, CPi, and CPm) is used for each of the sectors (the sector storing IS1/IS2, the sector storing IS(j-1), and the sector storing ISm), i.e., the allocated area of the chip card. In fact, an artisan would have understood that it would have been obvious to store the information IS1-IS2, IS(j-1), and ISm in sectors of the chip card (using different encryptions/decryption keys as suggested by Hazard), because chip cards are known to comprise storage sectors, and the artisan is a person of ordinary creativity, not an automaton. *See KSR*, 127 S. Ct. at 1742.

Though the Appellants argue that "sensitive information IS1 and IS2 of Hazard is encrypted using the same encryption key, 'CP1'," such argument is not commensurate the claimed invention. As discussed above, an artisan would have found it obvious that Hazard discloses, or at the least, strongly suggests, storing sensitive information IS1 and IS2 in a "sector" using encryption key CP1, which is different from the keys (CPi, CPm, etc) used by the other sectors of the chip card.

Accordingly, we find that Hazard discloses the claimed limitation of "a cryptosystem unit that selectively uses a different encryption key for each sector from the first sector to the M-th sector to execute encryption processing and the cryptosystem unit executes encryption processing on data to be stored in each of the sectors" (Claim 1).

B. The cited references disclose "revocation information regarding revoked media or content" and "a permission table that describes memory access control information".

Appellants further argue that "Sudia discloses privileges and authorizations that are granted to and revoked from a user," and that "[t]he privileges and authorizations are not granted to and revoked from media or content" (App. Br. 11). In particular, Appellants argue "the revoked privileges and authorizations do not constitute 'revoked media or content'"" (App. Br. 11). The Appellants add that, in Sudia, "[t]he block permission table does not 'lead[s] to various user rights'," but instead Sudia discloses "a 'permission table that describes memory access control information'" (App. Br. 11). Accordingly, the issue is whether Hazard discloses "a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information" (Claim 1).

As to "a revocation list having revocation information regarding revoked media or content," the Examiner finds that Sudia discloses this claimed limitation beginning at page 4 of the Answer, and provides corresponding responsive arguments beginning at page 15 of the Answer. In particular, the Examiner finds that "the phrase 'regarding revoked media or content' is broad and is therefore broadly interpreted" (Ans. 15), and that "the scope of the claim only requires that the list has information associated with the media or content that has been revoked, whether from one user or from a plurality of user" (Ans. 16). The Examiner explains "Sudia teaches that these revoked privileges are associated with content that the user may no longer access based on the revocation, hence revocation information regarding revoked content" (Ans. 16). We generally agree.

Sudia discloses controlling access to content governed by a given privilege, based on verification results (FF 5). In Sudia, a list is compiled containing all possible authorizations, restrictions that might ever be desired to be granted to or imposed on the user (FF 6). We find that Sudia discloses a list having revocation information, such as authorization or restriction information used to determine whether the client's access is refused (revoked) (FF 6), wherein access to content is controlled based on verification of the information (FF 5). Thus, we find the list of Sudia to be a revocation list having revocation information, such as authorization or restriction information, and the revocation information used to determine the client's access in Sudia to be information regarding revoked content.

We note that the feature "revocation" in "revocation list" and "revocation information" or "revoked" in "revoked content" is nonfunctional descriptive material that is not functionally related to the claimed information recording device. Such "revocation" or "revoked" feature does not change the functionality of or provide an additional function to the claimed device, but rather, are mere labels set forth for the list, information or content. When the descriptive material is not functionally related to the claimed embodiment, the descriptive material will not distinguish the invention from the prior art in terms of patentability. *See In re Ngai* at 1339 and *In re Gulack* at 1385.

As to "a permission table that describes memory access control information," the Examiner finds that Sudia discloses such claimed limitation beginning at page 4 of the Answer, and provides corresponding responsive arguments beginning at page 17 of the Answer. In particular, the Examiner finds that the Appellants' arguments "are not mentioned in the claims" (Ans. 17), and that "Sudia teaches the use of tables/lists that define which users are authorized to access various contents/resources held in various memory elements/locations based on the specific type of data at hand" (Ans. 18). Thus, Examiner finds "Sudia suggests using a block permission table for accessing a permission table that describes memory access information" (Ans. 18). We generally agree.

Sudia discloses creating a table of possible authorizations for a given user (FF 7), wherein access to data and network resources is governed by a given privilege, based on verification results (FF 5). We agree with the Examiner that the table of Sudia is permission table which describes memory access information since the table describes authorization information used to determine access.

We note that the feature "memory access" in "memory access information" is also a nonfunctional descriptive material that is not functionally related to the claimed information recording device, and does not change the functionality of or provide an additional function to the claimed device, but rather, are labels set forth for the information.

Accordingly, we conclude that Sudia discloses the claimed limitation of "wherein the data includes a revocation list having revocation information regarding revoked media or content and a block permission table for accessing a permission table that describes memory access control information" (Claim 1).

C. The cited references disclose an "integrity checking unit"

Appellants further argue that "Sudia does not disclose checking 'the integrity of the revocation list and block permission table'" (App. Br. 12). Accordingly, the issue is whether Sudia discloses "an integrity checking unit for checking the integrity of the revocation list and the block permission table" (Claim 1).

The Examiner's finds that Sudia suggests such claimed limitation beginning at page 4 of the Answer, and provides corresponding responsive arguments beginning at page 18 of the Answer. No evidence has been presented by the Appellants that is contrary to the Examiner's finding.

Sudia discloses, upon receipt of notification of revocation or suspension, a verifier is notified (FF 8) for verification. We find this verification to be a checking of the integrity of the revocation. Accordingly, we conclude that Sudia discloses "an integrity checking unit for checking the integrity of the revocation list and the block permission table" (Claim 1).

Thus, Appellants have not shown that the Examiner erred in finding that claims 1, 5, 8, 15-17, 24, 31, and 32 are unpatentable under 35 U.S.C. § 103(a).

Claims 5, 12, 16, 21, and 28

Appellants do not provide separate arguments with respect to the rejection of dependent claims 5, 12, 16, 21, and 28, depending from independent claims 1, 8, 15, 17, and 24, respectively. Thus, claims 5, 12, 16, 21, and 28 fall with claims 1, 8, 15, 17, and 24, and we conclude that the Appellants have not shown that the Examiner erred in rejecting claims 5, 12, 16, 21, and 28 under 35 U.S.C. § 103(a).

Claims 6, 13, 22, and 29

As to dependent claims 6, 13, 22, and 29, Appellants provide the same argument as independent claims 1, 8, 15, 17, and 24 from which they depend, and add the argument that "the Examiner does not rely upon, nor does Dilkie et al. disclose the deficiencies of Hazard and Sudia discussed above." (App. Br. 13).

We see no deficiencies regarding Hazard and Sudia, as discussed above regarding claims 1, 8, 15, 17, and 24. Therefore, we conclude that Appellants have not shown that the Examiner erred in rejecting claims 6, 13, 22, and 29 under 35 U.S.C. § 103(a).

CONCLUSION OF LAW

(1) Appellants have not shown that the Examiner erred in finding that claims 1, 5, 8, 12, 15-17, 21, 24, 28, 31, and 32 are unpatentable under 35 U.S.C. § 103(a) over the teachings of Hazard and Sudia.

(2) Appellants have not shown that the Examiner erred in finding that claims 6, 13, 22, and 29 are unpatentable under 35 U.S.C. § 103(a) over the teachings of Hazard, Sudia, and Dilkie.

(3) Claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32 are not patentable.

DECISION

The Examiner's rejection of claims 1, 5, 6, 8, 12, 13, 15-17, 21, 22, 24, 28, 29, 31, and 32 under 35 U.S.C. § 103(a) is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

pgc

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON DC 20001-4413